UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Snapchat Account User: falyc0, phone number (206) 434-0585, email address feylacow@outlook.com, IP Address 107.116.255.98, more fully described in Attachment A.	)	Case No. MJ24-512

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Snapchat Account User: falyc0, phone number (206)434-0585, email address feylacow@outlook.com, IP Address 107.116.255.98, more fully described in Attachment A.

located in the Southern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2256(8)	Possession of Child Pornography

The application is based on these facts:

✓ See Affidavit of Special Agent Andrew Butler, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Andrew Butler, Special Agent (FBI)

Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or

◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 08/21/2024

Judge's signature

City and state: Seattle, Washington

S. Kate Vaughan, United States Magistrate Judge

Printed name and title

USAO: 2024R00676

AFFIDAVIT OF SPECIAL AGENT ANDREW BUTLER

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

AFFIANT BACKGROUND

1. I, Andrew Butler, a Special Agent with the Federal Bureau of Investigation ("FBI") in Seattle, Washington, having been first duly sworn, hereby depose and state as follows:

INTRODUCTION AND PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of an application for a search warrant for information associated with certain Snapchat accounts that are stored at premises owned, maintained, controlled, or operated by Snap, Inc. ("Snapchat"), a company headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Snapchat to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account.

3. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since October 2019. Prior to this assignment I was an Infantry Officer in the United States Army. I am currently assigned to the Seattle Field Office in Seattle, Washington and serve on the FBI Seattle Child Exploitation and Human Trafficking Task Force and as a member of the Washington State Internet Crimes Against Children (ICAC) Task Force. As an FBI Special Agent, I investigate criminal violations relating to child exploitation and human trafficking, including violations pertaining to the commercial sexual abuse of minors and adults, and the online sexual exploitation of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

children involving the transmission, possession and production of child pornography, exploitation of children on the internet, as well as other federal criminal activity and attempts or conspiracies to commit those crimes. I have received specialized training from the FBI Academy consisting of legal classes, criminal procedure, investigative techniques, evidence preservation and collection, and other law enforcement training classes. Through my training and experience, I have developed an understanding of common habits and practices used by those engaged in criminal acts against children and those who facilitate the commercial sex trafficking of minors and adults. I have participated in investigations involving the analysis of Internet Protocols (IPs) and exploitation of social media accounts.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2423(b) Travel with the Intent to Engage in a Sexual Act with a Minor, Attempted Enticement of a Minor in violation of Title 18, United States Code, Section 2422(b), and violations of Title 18 United States Code Sections 2251(a) and (e), 2252(a)(2), Production and Receipt of Child Pornography were committed by Snapchat user halyc0n. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

DEFINITIONS

The following definitions apply to this affidavit:

6. "Chat," as used herein, refers to any kind of text communication over the internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as internet forums and email.

7. For the purposes of this affidavit, a "minor" refers to any person less than eighteen years of age and for the purpose of this search warrant, "Child pornography," as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

8. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

9. "Cloud-based storage service," as used herein, refers to a publicly accessible, online storage provider that collectors of depictions of minors engaged in sexually explicit conduct can use to store and trade depictions of minors engaged in sexually explicit conduct in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders or collectors of depictions of minors engaged in sexually explicit conduct in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

10. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device," including smartphones and mobile devices.

11. "Data," as used herein refers to the quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.

12. "Digital Devices" as used herein refers to any physical object that has a computer, microcomputer, or hardware that is capable of receiving, storing, possessing, or potentially sending data.

13. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

14. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations, community-owned, non-profit, or otherwise privately-owned companies that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

15. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

16. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

17. "User Attributes," as used herein refers to any tangible data, documents, settings, programs, or other information that provides information related to the identity of the specific user of the device, computer, application, program, or record.

BACKGROUND

Based on my training, experience and collaboration with other law enforcement officers that investigate child exploitation, as well as industry experts, academia and other service providers, I know the following:

18. That adult persons with a sexual interest in minors are persons whose sexual targets are children. They receive sexual gratification and satisfaction from actual physical contact with children, fantasy involving the use of writings detailing physical contact with children, and/or from fantasy involving the use of pictures and/or videos of minors.

19. The development of the computer has changed the way children are engaged in sexually explicit conduct and the files created therefrom are distributed thereafter. The computer serves four functions in connection with depictions of children engaged in sexually explicit conduct. These four functions include: production, communications, distribution, and storage.

20. Pornographers produce both still and moving images, i.e.: photographs and video. These files can be transferred either directly from the camera/camera phone into a computer or mobile application, directly from a storage device such as a flash drive to a computer, or the image files can be transferred directly into the computer by use of a scanner.

21. In addition to data sharing between phones, mobile and desktop applications, and websites, e-mail may also be used electronically transmits files through a user's electronic device.

22. All that a smart phone or computer user needs to do in order to use an application, website, or email is open up an account with one of the myriad of companies

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

that provide services (e.g. Meta, Microsoft, Google, Discord, Snapchat, Dropbox, etc.). Once the account is set up, the user can choose the "name" of his/her account, which does not have to match (or even relate to) identifying information of the user. Thus, the user name by itself does nothing to identify the owner of the account, the user, or the composer of the communication. Nevertheless, often times the communications themselves, contain information that either directly or indirectly identifies the composer of the file. Based on my training and experience investigating child exploitation offenses, I know it is common for collectors of depictions of minors engaged in sexually explicit conduct to use multiple social media accounts and/or applications in order conceal their true identity and/or more easily categorize their collection according to the type of material or source.

23. Individuals involved in computer-related crimes often use these accounts to conduct both criminal and non-criminal communications. Consequently, these communications can be a great source of information to help identify the sender and/or recipient of the file and/or message. The ability to view these communications by investigating law enforcement often provides further investigative leads to assist in identifying the person of interest.

24. I know that an Internet Protocol (IP) address is a numerical label assigned to devices communicating on the internet and that the Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally. An IP address provides the methodology for communication between devices on the internet. It is a number that uniquely identifies a device on a computer network and, using transport protocols, moves information on the internet. Every device directly connected to the internet must have a unique IP address.

25. An IP address is typically comprised of four (4) series of numbers separated by periods and is most commonly represented as a 32-bit number such as

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

71.227.252.216 (Internet Protocol Version 4). IPv6 is deployed as well and is represented as a 128-bit number such as 2001:db8:0:1234:0:567:8:1.

26. IP addresses are owned by the Internet Service Provider and leased to a subscriber/customer for a period of time. They are public and visible to others as you surf the internet. The lessee has no expectation of privacy due to the public nature of IP addresses.

27. When an Internet Service Provider's customer logs onto the internet using a computer or another web-enabled device, they are assigned an Internet Protocol (IP) address.

28. There are two different types of Internet Protocol addresses. The first is a dynamic IP address, which means the user's IP address may change each time they log on to the internet. The frequency in which this address changes is generally controlled by the Internet Service Provider and not the user. The other type of IP address is a static IP address, which means that a user is assigned a specific IP address that remains constant every time they log on to the internet.

29. IP addresses are similar to a license plate on a motor vehicle. They are the property of the issuer, and not the vehicle owner. Just as your license plate is visible as you cruise your city or town, your IP address is visible as you cruise the internet. Your IP address is visible to the administrators of websites you visit, attached emails you send, and broadcast during most internet file and information exchanges that occur on the internet.

30. I know based on my training and experience, that Electronic Service Providers ("ESP") and/or Internet Service Providers ("ISP," collectively ISP) typically monitor their services utilized by subscribers. To prevent their communication networks from serving as conduits for illicit activity and pursuant to the terms of user agreements, ISPs routinely and systematically attempt to identify suspected depictions of minors engaged in sexually explicit conduct that may be sent through its facilities. Commonly,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

customer complaints alert them that an image or video file being transmitted through their facilities likely contains suspected depictions of minors engaged in sexually explicit conduct.

31. When an ESP/ISP receives such a complaint or other notice of suspected depictions of minors engaged in sexually explicit conduct, they may employ a "graphic review analyst" or an equivalent employee to open and look at the image or video file to form an opinion as to whether what is depicted likely meets the federal criminal definition of depictions of minors engaged in sexually explicit conduct found in 18 USC § 2256, which is defined as any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. If the employee concludes that the file contains what appears to be depictions of minors engaged in sexually explicit conduct, a hash value of the file can be generated by operation of a mathematical algorithm. A hash value is an alphanumeric sequence that is unique to a specific digital file. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, results in a different hash value. Consequently, an unknown image can be determined to be identical to an original file if it has the same hash value as the original. The hash value is, in essence, the unique fingerprint of that file, and when a match of the "fingerprint" occurs, the file also matches. Several different algorithms are commonly used to hash-identify files, including Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

32. Hash values are a very reliable method of authenticating files. It can be concluded with an extremely high degree of certainty that two files sharing the same hash value also share identical content. Based on my training and experience, as well as others in this field, I know it is more likely that two humans would share the same biological DNA than for two files to share the same hash value. If even one bit (the smallest measure of data in a file) of a file is changed, the entire hash value of that file changes completely. As an example that demonstrates the uniqueness of a SHA-1 hash, the likelihood of two files having the same SHA-1 hash value is 2^{128} or:1 in 340,000,000,000,000,000,000,000,000,000,000,000,000 chance. In an August 6th, 2020 article in Live Science[1], according to Professor Simona Francese, PhD, a forensic scientist and fingerprint expert from Sheffield Hallam University in the United Kingdom, the likelihood of two humans having the same fingerprint is estimated to be:1 in 64,000,000,000.[2]

33. For two different files to have the same hash value is called a *collision.* I know from experience that there have been no documented incidents of a collision involving SHA-1 hash values "in the wild" since its creation in 1995. I am, however, aware of a reported collision involving two files sharing the same SHA-1 value in a lab setting. This was done purposely by engineers at Google[3] in 2017 under controlled conditions for the sole purpose of creating this collision. Even with this knowledge in mind, I am confident that the possibility of a suspected child sexual abuse material file reported in a CyberTip having the same hash value as an unrelated, non-criminal file is extremely unlikely. I believe hash value comparison is a highly reliable method of

---

[1] Baker, Harry. "Do Identical Twins Have Identical Fingerprints?" LiveScience, Purch, 7 Aug. 2021, https://www.livescience.com/do-identical-twins-have-identical-fingerprints.html.

[2] Of note, in the same article, Professor Francese, who is a peer-reviewed, published scientist, commented, "to this day, no two fingerprints have been found to be identical."

[3] "Announcing the First sha1 Collision." *Google Online Security Blog*, 23 Feb. 2017, https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

determining if two files are the same or different, and that a confirmed hash match between two files is a forensic finding on a par with a DNA match or a fingerprint match.

34. ESPs typically maintain a database of hash values of files that they have determined to meet the federal definition of depictions of minors engaged in sexually explicit conduct found in 18 USC § 2256. The ISPs typically do not maintain the actual suspect files themselves; once a file is determined to contain suspected depictions of minors engaged in sexually explicit conduct, the file is deleted from their system.

35. The ESPs can then use Image Detection and Filtering Process ("IDFP"), Photo DNA (pDNA), or a similar technology which compares the hash values of files embedded in or attached to transmitted files against their database containing what is essentially a catalog of hash values of files that have previously been identified as containing suspected depictions of minors engaged in sexually explicit conduct.

36. When the ESP detects a file passing through its network that has the same hash value as an image or video file of suspected depictions of minors engaged in sexually explicit conduct contained in the database through a variety of methods, the ISP reports that fact to National Center for Missing and Exploited Children (NCMEC) via the latter's CyberTipline. By statute, an ESP or ISP has a duty to report to NCMEC any apparent depictions of minors engaged in sexually explicit conduct it discovers "as soon as reasonably possible." 18 U.S.C. § 2258A(a)(1). The CyberTip line report transmits the intercepted file to NCMEC. Often that occurs without an ISP employee opening or viewing the file because the files hash value, or "fingerprint," has already been associated to a file of suspected depictions of minors engaged in sexually explicit conduct. The ISP's decision to report a file to NCMEC is made solely on the basis of the match of the unique hash value of the suspected depictions of minors engaged in sexually explicit conduct to the identical hash value in the suspect transmission.

37. ESP's also monitor which devices are used to access their platform by recording the advertising identification number. This number is a unique identifier

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

assigned to hardware devices used by ESP's to track users semi-anonymously and provide targeted advertisements. Because it is a unique identifier, this information can link specific devices owned by specific individuals with the criminal activity on a particular platform's account.

38. Most Internet Service Providers keep subscriber records relating to the IP address they assign, and that information is available to investigators. Typically, an investigator has to submit legal process (e.g. subpoena or search warrant) requesting the subscriber information relating to a particular IP address at a specific date and time.

39. A variety of publicly available websites provide a public query/response protocol that is widely used for querying databases in order to determine the registrant or assignee of internet resources, such as a domain name or an IP address block. These include WHOIS, MaxMind, arin.net, and other common search tools.

40. The act of "downloading" is commonly described in computer networks as a means to receive data to a local system from a remote system, or to initiate such a data transfer. Examples of a remote system from which a download might be performed include a webserver, FTP server, email server, or other similar systems. A download can mean either any file that is offered for downloading or that has been downloaded, or the process of receiving such a file. The inverse operation, "uploading," refers to the sending of data from a local system to a remote system such as a server or another client with the intent that the remote system should store a copy of the data being transferred, or the initiation of such a process.

41. The National Center for Missing and Exploited Children (NCMEC) is a private, non-profit organization established in 1984 by the United States Congress. Primarily funded by the Justice Department, the NCMEC acts as an information clearinghouse and resource for parents, children, law enforcement agencies, schools, and communities to assist in locating missing children and to raise public awareness about

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ways to prevent child abduction, child sexual abuse and depictions of minors engaged in sexually explicit conduct.

42. The Center provides information to help locate children reported missing (by parental abduction, child abduction, or running away from home) and to assist physically and sexually abused children. In this resource capacity, the NCMEC distributes photographs of missing children and accepts tips and information from the public. It also coordinates these activities with numerous state and federal law enforcement agencies.

43. The CyberTipline offers a means of reporting incidents of child sexual exploitation including the possession, manufacture, and/or distribution of depictions of minors engaged in sexually explicit conduct; online enticement; child prostitution; child sex tourism; extra familial child sexual molestation; unsolicited obscene material sent to a child; and misleading domain names, words, or digital images.

44. Any incidents reported to the CyberTipline online or by telephone go through this three-step process: CyberTipline operators review and prioritize each lead; NCMEC's Exploited Children Division analyzes tips and conducts additional research; The information is accessible to the FBI, ICE, and the USPIS via a secure Web connection. Information is also forwarded to the ICACs and pertinent international, state, and local authorities and, when appropriate, to the ESP.

45. Based upon my knowledge, experience, and training in depictions of minors engaged in sexually explicit conduct investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in depictions of minors engaged in sexually explicit conduct:

a. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct may collect sexually explicit or suggestive materials in a variety of media, including photographs and videos. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

d. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other depictions of minors engaged in sexually explicit conduct distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in depictions of minors engaged in sexually explicit conduct.

e. Those that possess, receive and attempt to receive depictions of minors engaged in sexually explicit conduct prefer not to be without their depictions of minors engaged in sexually explicit conduct for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of depictions of minors engaged in sexually explicit conduct throughout the world.

46. Based on my training and experience, collectors and distributors of depictions of minors engaged in sexually explicit conduct also use online, remote, resources to retrieve and store depictions of minors engaged in sexually explicit conduct, including services offered by many companies for cloud-storage and digital

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

communications. The online services allow a user to set up an account with a remote computing service that provides email services and/or electronic storage of electronic files in any variety of formats. A user can set up, and access, an online storage account from any computer or digital device with access to the internet. Evidence of such online storage of depictions of minors engaged in sexually explicit conduct is often found on the user's computer or smart phone. Even in cases where online storage is used, however, evidence of depictions of minors engaged in sexually explicit conduct can be found on a user's digital device if that device is used to access the internet. Cloud storage allows the offender ready access to the material from any device that has an internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender's device. Evidence located in cloud storage may be deleted from any device capable of reaching the website of the cloud hosting company. Once the individual user credentials, often a username and password are entered, the data in the cloud storage may be accessed, modified, shared, or deleted. Unlike deleting data from a local hard drive, once data is deleted from cloud storage, it is wiped from the cloud hosting company's servers and is unrecoverable.

47. In addition to the traditional collector, law enforcement has encountered offenders who obtain depictions of minors engaged in sexually explicit conduct from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification.

48. Additionally, offenders may opt to store the contraband in cloud accounts. Cloud storage is a model of data storage where the digital data is stored in logical pools,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the physical storage can span multiple servers, and often locations, and the physical environment is typically owned and managed by a hosting company. Cloud storage allows the offender ready access to the material from any device that has an internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender's device.

49. Based on my training and experience and my consultation with computer forensic detectives and agents who are familiar with searches of computers and smartphones, I have learned that offenders will try and obfuscate data containing images and videos of minors engaged in sexual activity. One potential manner of trying to hide the contraband may be by changing file extensions. For example, an image file may often have a file extension of ".jpg" of ".jpeg" signifying that it is an image or photograph. An offender may change the file extension by selecting the "save as" format on a computer or digital device and select ".doc" or ".docx" to make it appear that instead of a contraband image or photograph, it is a word document. The same process may be used to attempt to hide a video file as well. Based on these, and other attempts to hide potential contraband is necessary for forensic examiners to examine all potential data on a digital device.

50. I know that, regardless of whether a person discards or collects depictions of minors engaged in sexually explicit conduct he accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of depictions of minors engaged in sexually explicit conduct, backup files, and other electronic artifacts that may be forensically recoverable.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

BACKGROUND CONCERNING SNAP INC. (Snapchat)[4]

51. Snapchat is a popular social media platform used for posting short videos, photos, memes, text messages and other electronic content. Like Facebook, Instagram, and other social media sites, posted content can be shared with your "friends" on the platform. The user has the option to share posts and/or communicate with their friends individually or with their entire friend group through "My Story." Public posts made on "My Story" can be viewed for 24 hours before they disappear.

52. In my professional experience, having talked to other detectives that have investigated cases involving the use of Snapchat and have received historical data from previously written Snapchat warrants, I know that data stored in Snapchat user accounts, to include photos, videos, memes, instant message exchanges, geolocation data, and user information, provides valuable supporting evidence in criminal investigations.

53. Service Provider Identity: I have confirmed that the service provider receives and processes legal requests at: Snap Inc., ATTN: Custodian of Records, 2772 Donald Douglas Loop North, Santa Monica, CA 90405, lawenforcement@snapchat.com.

54. Service Provider Records: Subscriber information (often known as "registration information" for Internet applications or service) is obtained by the service provider when an account is established and typically includes information such as: The subscriber name, address, billing/payment information; account initiation date; changes to the account; type of account; custom account features; additional phone numbers, email addresses, and/or other contact information; additional persons having authority on the account; any additional accounts linked to the subject account; and unique identifiers for the device using the target address, and other devices the customer of the subject account uses. In my experience, this information frequently provides investigative leads.

---

[4] The information in this section is based on information published by Snapchat's "Privacy Policy" website, including, but not limited to, the following webpages: "Privacy Policy available at https://values.snap.com/privacy/privacy-policy, as well as the Snapchat Law Enforcement Guide.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

55. The following in an excerpt from Snapchat's website discussing the types of information they collect:

Information We Get When You Use Our Services

When you use our services, we collect information about which of those services you've used and how you've used them. We might know, for instance, that you watched a particular Story, saw a specific ad for a certain period of time, and sent a few Snaps. Here's a fuller explanation of the types of information we collect when you use our services:

Usage Information. We collect information about your activity through our services. For example, we may collect information about:

- *how you interact with our services, such as which filters you view or apply to Snaps, which Stories you watch on Discover, whether you're using Spectacles, or which search queries you submit.*
- *how you communicate with other Snapchatters, such as their names, the time and date of your communications, the number of messages you exchange with your friends, which friends you exchange messages with the most, and your interactions with messages (such as when you open a message or capture a screenshot).*
- *Content Information. We collect content you create on our services, such as custom stickers, and information about the content you create or provide, such as if the recipient has viewed the content and the metadata that is provided with the content.*
- *Device Information. We collect information from and about the devices you use. For example, we collect:*
- *information about your hardware and software, such as the hardware model, operating system version, device memory,*

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

advertising identifiers, unique application identifiers, apps installed, unique device identifiers, browser type, language, battery level, and time zone;

- *information from device sensors, such as accelerometers, gyroscopes, compasses, microphones, and whether you have headphones connected; and*
- *information about your wireless and mobile network connections, such as mobile phone number, service provider, IP address, and signal strength.*
- *Device Phonebook. Because Snapchat is all about communicating with friends, we may—with your permission—collect information from your device's phonebook.*
- *Camera and Photos. Many of our services require us to collect images and other information from your device's camera and photos. For example, you won't be able to send Snaps or upload photos from your camera roll unless we can access your camera or photos.*

Location Information. When you use our services we may collect information about your location. With your permission, we may also collect information about your precise location using methods that include GPS, wireless networks, cell towers, Wi-Fi access points, and other sensors, such as gyroscopes, accelerometers, and compasses.

Information Collected by Cookies and Other Technologies. Like most online services and mobile applications, we may use cookies and other technologies, such as web beacons, web storage, and unique advertising

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

identifiers, to collect information about your activity, browser, and device. We may also use these technologies to collect information when you interact with services we offer through one of our partners, such as advertising and commerce features. For example, we may use information collected on other websites to show you more relevant ads. Most web browsers are set to accept cookies by default. If you prefer, you can usually remove or reject browser cookies through the settings on your browser or device. Keep in mind, though, that removing or rejecting cookies could affect the availability and functionality of our services. To learn more about how we and our partners use cookies on our services and your choices, please check out our Cookie Policy.

Log Information. We also collect log information when you use our website, such as:

- *details about how you've used our services;*
- *device information, such as your web browser type and language;*
- *access times;*
- *pages viewed;*
- *IP address;*
- *identifiers associated with cookies or other technologies that may uniquely identify your device or browser; and*
- *pages you visited before or after navigating to our website.*
- *Information We Collect from Third Parties*

We may collect information about you from other users, our affiliates, and third parties. Here are a few examples:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

- *If you link your Snapchat account to another service (like Bitmoji or a third-party app), we may receive information from the other service, like how you use that service.*
- *Advertisers, app developers, publishers, and other third parties may share information with us as well. We may use this information, among other ways, to help target or measure the performance of ads. You can learn more about our use of this kind of third-party data in our Support Center.*
- *If another user uploads their contact list, we may combine information from that user's contact list with other information we have collected about you.*

SUMMARY OF PROBABLE CAUSE

Snapchat Username Halyc0n

56. The United States is investigating violations of Travel with the Intent to Engage in a Sexual Act with a Minor and has secured an Indictment in this case against NEWCOMER for violations of, inter alia, Title 18 United States Code 2423(b). This warrant application seeks to investigate possible violations of Title 18 United States Code, Sections 2252(a)(4)(B),(b)(2), Possession of Child Pornography stemming from a cybertip generated by SnapChat and reported to the National Center for Missing and Exploited Children involving username falyc0, which is an account associated with NEWCOMER's Halyc0n SnapChat account based upon my review of the search warrant return data obtained by Snoqualmie Police Department during their investigation detailed below.

2020 Rape of a Child Third Degree – Two Counts – King County Superior Court

57. JAMES HARRISON NEWCOMER aka JAKE HARRISON NEWCOMER birth year 1996 was convicted of two counts of Rape of a Child in the Third Degree following his sexual assault of a 15-year-old female victim between July 24, 2020, and July 27, 2020. That investigation revealed that NEWCOMER, then 24 years old, reported

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to the victim that he was 17 years old when he added the victim on Snapchat. After interacting with the victim for less than 24 hours, NEWCOMER drove from King County, Washington to Clallam County, Washington and picked the victim up near a bed and breakfast where she was visiting with her family. NEWCOMER drove for approximately five minutes, pulled over the vehicle at an unknown area, and sexually assaulted the victim orally and vaginally.

58. NEWCOMER provided the victim with alcohol and marijuana and drove the victim to his parent's King County residence where he resided. He snuck the victim into his parent's home and sexually assaulted her approximately ten times over several days before she was recovered at his parent's residence by law enforcement on July 27, 2020.

59. After serving 30 months in prison, NEWCOMER was under conditions of Community Custody with the Department of Corrections (hereafter DOC) and was required to register as a sex offender. Pursuant to the terms of NEWCOMER's community custody he was required to wear an ankle monitor. On January 19, 2024, NEWCOMER's ankle monitor died and lost connection. On January 25, 2024, Washington DOC attempted to arrest NEWCOMER at his residence, but were unable to locate him. Washington DOC entered an arrest warrant for NEWCOMER following the ankle monitor battery dying and NEWCOMER's unknown location. On June 7, 2024, NEWCOMER was arrested in Kent, Washington and is currently in custody for his DOC violations.

MINOR VICTIM 1: Snoqualmie Police Department – February 2024

60. On or about February 8, 2024, I was contacted by Snoqualmie Police Department Officer Aguirre about a missing 16-year-old female MINOR VICTIM DOB 2007 (hereinafter MV1). Within several hours of the notification, MV1 returned home. A subsequent Snoqualmie Police Department investigation discovered that MV1 was picked up at her North Bend residence and provided narcotics by an adult male identified

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

by Snapchat username "Halyc0n." Specifically, investigators learned that MV1 was added on Snapchat by halyc0n, who picked up MV1 from her North Bend, Washington residence at approximately 1:00 a.m. on February 7, 2024, and was driven to an apartment in the Seattle, Washington where halyc0n provided MV1 methamphetamine. A toxicology screening was subsequently administered to MV1 and yielded positive result for methamphetamine. Halyc0n drove MV1 back home on February 8, 2024, at approximately 8:00am.

61. A neighbor observed a black Toyota sedan drop MV1 off in the vicinity of her residence and attempted to follow the vehicle. The neighbor observed the black Toyota sedan did not have license plates. MV1's mother, (hereafter MOTHER1), reported that she viewed photos, videos, and messages between MV1 and halyc0n which confirmed sexual intercourse occurred.

62. On February 9, 2024, MV1 was forensically interviewed. MV1 disclosed that she was added on Snapchat by halyc0n and met in person with him the same day. MV1 described halyc0n as a 28-year-old male and her relationship with him as romantic. MV1 confirmed she was picked up by halyc0n, whom she called "J" on February 7, 2024, at approximately 0100 PST and was taken to his Seattle apartment where she met his adult roommate and roommate's adult girlfriend. "J" instructed MV1 to claim she was 18 years old so she did not become suspicious to the roommates' adult girlfriend. As detailed below, investigators subsequently confirmed the identity of Snapchat user halyc0n as NEWCOMER.

63. The Snoqualmie Police Department, Officer Aguirre obtained a search warrant for Snapchat user halyc0n. Review of the return provided by Snapchat included subscriber information for Snapchat user halyc0n. Subscriber information included phone number (206)434-0585, reported date of birth July 26, 2007, email address feylacow@outlook.com, and associated username falyc0.

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

MINOR VICTIM 2: Auburn Police Department – February 2024

64. During the course of the Snoqualmie Police Department investigation, I learned of a similar Auburn Police Department case involving Snapchat username "halyc0n." On February 22, 2024, Auburn Police Department was notified that MINOR VICTIM 2 DOB 2008 (hereafter MV2 2008) ran away overnight. MV2's mother (hereafter MOTHER2) reporting having viewed MV2's laptop and observing Snapchat messages between MV2 and Snapchat username halyc0n. Halyc0n's messages to MV2 detailed how MV2 could disable the security alarm on her window and instructed MV2 to wait until her parents go to sleep before leaving. Halyc0n reported he would be waiting to pick MV2 up and expressed plans to get MV2 a fake identification card that reported MV2 to be 18 years old instead of 15 years old. The Snapchat messages detailed the intention behind the fake identification card would be to allow MV2 to gain access to online pornographic websites where videos of sexual contact between MV2 and halyc0n could be uploaded to make money.

65. Described below in relevant part, are two Snapchat communications send from halyc0n to MV2:

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. "You know. Just for the record. I would be more inclined. to take you away forever. If I knew there would be money coming in. Now obviously I would never pimp you out sweetpea. you belong to me. and only me. but. There ARE things. That dont involve you being in any. situation with other real people. That could male some living money pretty easily. but they are only things I could set up to do with you. If I had you around all the time. Like we could get on cam together."

b. "Get you a fake ides. ID. And we could go be "legal loli porn. on a cam site. we would rake it in savagely. Because of your size. and because the company would think you were 18. Because of the fake ID. So if you want to get out sooner. Perhaps you should think on that. But it cant really be like. Okay Ill do it.and then I take you. And you puss out at the last second. Cause if that money doesnt come through from somewhere to pay for you to have what you need. You and I are BOTH fuckdc. fucked. So if you decide you wouldn't mind fucking on camera with me. Perhaps you could leave sooner than I thought. Just a thoughr. thought.* Cammers make a lot of money. plus by camming. you open up the ability to sell. if you wish. which is a business that runs itself. lol. Your tiny body is actually worth a lot of money. without even having to touch anyone. Or actually see them. Something to consider."

66. I know based on my training and experience that the term "loli" is used by adults who have a sexual interest in children. The term is jargon and encompasses the genre of adults who have a sexual interest in children and Child Sexual Abuse Material (CSAM).

67. MV2 disclosed to investigators that she received a Snapchat message from a user identified as "Aiden" in June 2023. In September 2023, MV2 sent "Aiden" two fully nude photographs of herself via Snapchat and to visiting "Aiden's" two-bedroom apartment in Seattle, where he lived with a roommate. MV2 stayed in one room at the apartment and the roommate in another. MV2 reported communicating with "Aiden." I reviewed the data returned by Snapchat for halyc0n's account, obtained by a search warrant executed by Snoqualmie Police Department relating to the investigation involving MV1. I observed Snapchat user halyc0n was in fact in communication with MV2 on February 4, 2024. It is unclear if MV2 was protecting halyc0n or failed to accurately recall his username when speaking with law enforcement.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

68. During a Child and Adolescent Forensic Interview of MV2 on June 24, 2024, MV2 disclosed that MV2 was picked up from their house by a male identified as Josh in May 2024. MV2 stated Josh picked them up in a black vehicle. MV2 admitted they had communicated with Josh since the summer of 2023. I know from Pierce County Sheriff's Department report 2414901148, MV2 was reported missing from her residence by MOTHER2 on May 19, 2024. Jennifer reported she suspected that MV2 ran away with someone she met online via Snapchat.

69. On June 13, 2024, Des Moines Police Department recovered MV2 after a hotel employee of the Legend Motel, 22204 Pacific Highway South Des Moines, Washington, reported a suspicious circumstance that involved an adult male, an adult female and a suspected juvenile female. The subsequent Des Moines Police Department investigation identified that the suspected juvenile was MV2, who was with Jason MORRISON and Sherry RABAGO. MORRSION was also a registered sex offender and a known associate of NEWCOMER. MORRISON was arrested by Washington Department of Corrections on a violation of the terms of his supervision as a registered sex offender. RABAGO was interviewed by Des Moines Police Department and reported MV2 was only known to her as Jasper. I know based on the investigation to date that MV2 used Snapchat username ThingOnejasper and Jasper137137.

70. RABAGO further reported to Des Moines Police Department NEWCOMER was also present with herself, MV2, and MORRISON. MV2 was taken into custody by the Des Moines Police Department on June 13, 2024.

71. MV2 reported during a subsequent child forensic interview on June 24, 2024, that she was with the male identified as "Josh" until his arrest on approximately June 7, 2024.[5]

---

[5] During the course of the initial investigation, MV2 stated "they" (presumably herself, RABAGO, and MORRISON), were picked up by an individual identified as "Josh." Based on the forensic interview of MV2 and her disclosure of having been picked up by "Josh" in a black vehicle, "Josh" is believed by law enforcement to be an alias used by NEWCOMER. I know from the investigation to date that NEWCOMER drives a black 2011 Toyota

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

MINOR VICTIM 3: Woodburn Police Department – April 2024

72. On or about May 15, 2024, I contacted FBI Special Agent Chelsea Barker about subject Snapchat user "halyc0n." I learned from Special Agent Barker that a sexual assault involving a subject Snapchat user "halyc0n" occurred in Woodburn, Oregon. Woodburn Police Department investigated a report that a 14-year-old MINOR VICTIM DOB 2009 (hereafter MV3), had been sexually assaulted by an adult man in the Salem, Oregon area. Woodburn Police detectives obtained a search warrant for MV3's Snapchat records and observed that MV3 interacted with Snapchat user "halyc0n." Described below in relevant part, are Snapchat communications from halyc0n to MV3:

April 6, 2024, 3:49am "halyc0n" to MV3 via Voice Note: "…We're hanging out. We're fucking. I promise…"

April 9, 2024, 3:18am "halyc0n" to MV3 via Voice Note: "I can come right now. It' going to be about 2 hours and 15 minutes."

April 10, 2024, 12:09am "halyc0n" to MV3 via Snapchat text: Jpeg image of screenshot of phone navigation. Depicts vehicle headed south on WA-507 S near 92 AV S and 342nd Street S with an ETA of 3:20am.

April 10, 2024, 3:43am MV3 to "halyc0n" via Snapchat text: "Are u here"

April 10, 2024, 3:46am "halyc0n" to MV3 via Voice Notes: I'm in a Black Toyota Camry and I'm about to be at the address.

73. Woodburn Police Department reviewed Snapchat messages between MV3 and halyc0n on April 12, 2024. In those messages Woodburn Police Department investigators observed messages by halyc0n, which described having sex with MV3 in his vehicle. Halyc0n stated he bought privacy screens and mentioned they would have sex in an area near Walmart. Halyc0n detailed sexual acts he planned to perform on MV3, which included vaginal, oral and anal sexual penetration. MV3 shared plans of

---

Camry, bearing Washington license plate CES6678. Additionally, RABAGO reported to DMPD that NEWCOMER was present with herself and MV2 during the timeframe MV2 was missing.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

running away from home with halyc0n, who in turn expressed his willingness to assist her.

74. During a subsequent interview with law enforcement, MV3 disclosed that on April 10, 2024, a male from Washington identified as "Jack" picked her up. MV3 recalled the male listed his age as 16 years old on his Yubo social media. MV3 described being sexually assaulted in a Walmart parking lot by "Jack" to include vaginal and anal penetration. "Jack's" vehicle did not have license plates because the police were after him.

75. MV3 disclosed that "Jack" picked her up again on April 12, 2024, after she snuck out of the house. "Jack" drove to a Super 8 Hotel in Woodburn, Oregon where he sexually assaulted MV3 to include vaginal and oral penetration.

76. On May 15, 2024, Snoqualmie Police Department Officer Aguirre sent a request for information via email to law enforcement officers and prosecutors in the greater Seattle, Washington area. Included in the request for information were subject identifiers for Snapchat user halyc0n and photographs of Snapchat user halyc0n. Photographs of subject halyc0n were provided to law enforcement by MV1's parents. Photographs included in the request for information email were identified to be NEWCOMER by Washington DOC Community Corrections Officer Bullard, who supervised NEWCOMER following his sex offense convictions. Through interagency coordination between Snoqualmie Police Department, Woodburn Police Department, Washington DOC, and the FBI, Woodburn Police Department identified the male that picked up MV3 on April 10, 2024, and April 12, 2024, was NEWCOMER.

NCMEC Cybertip 192528710

77. As detailed above, the Snoqualmie Police Department obtained a search warrant for Snapchat user halyc0n. The return provided by Snapchat included subscriber information for Snapchat user halyc0n. Subscriber information included phone number (206)434-0585, reported date of birth July 26, 2007, email address

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

feylacow@outlook.com, and associated username falyc0. On June 24, 2024, I requested NCMEC query its databases for Cybertips associated to Snapchat usernames: Halyc0n, Falyc0; email address feylacow@outlook.com; and phone number (206)434-0585.

78. NCMEC reported that Cybertip 192528710 was associated and matched the identifiers included for uploading suspected Child Sexual Abuse Material to Snapchat. Snapchat username falyc0 uploaded one file of suspected Child Sexual Abuse Material to Snapchat on April 24, 2024. Based on the geolocation of the IP Address of the upload, NCMEC forwarded the Cybertip report to Seattle Police Department. After learning this information from NCMEC, SA Butler contacted Seattle Police Department to request a copy of the Cybertip. The Cybertip included the following identifiers: phone number (206)434-0585, reported date of birth July 26, 2007, email address feylacow@outlook.com, associated username falyc0, IP Address 107.116.255.98 which resolved to Seattle-Tacoma, Washington.

79. SA Butler reviewed the video Snapchat reported to NCMEC that contained suspected Child Sexual Abuse Material after having confirmed Snapchat reviewed the suspected CSAM. The video is depicted a pre-pubescent minor female, approximately 10 years to 12 years old, masturbating with a toothbrush. The minor female is seen laying on her back with her legs spread, fully nude, with the camera's view of her vagina and anus. The minor female masturbates and penetrates her vagina with the toothbrush. The minor female's bare chest and face are observed from the camera's point of view. The minor female does not have evidence of pubic hair and lacks breast development, both consistent with puberty. The minor female's face lacks development of facial features and body size of an adult female. I have viewed this file and based on my training and experience, I believe the file described above meet the federal definition of child pornography, as defined in 18 U.S.C. 2256(8).

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

80. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Snapchat to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

81. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Snapchat. Because the warrant will be served on Snapchat, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

82. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

83. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

Andrew Butler, Affiant
Special Agent, Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone on this 21st day of August, 2024.

THE HON. S. KATE VAUGHAN
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Snapchat Account username **falyc0, phone number (206)434-0585, reported date of birth July 26, 2007, email address feylacow@outlook.com, IP Address 107.116.255.98** that is stored at premises owned, maintained, controlled, or operated by Snap, Inc, a company headquartered in Santa Monica, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Snapchat

To the extent that the information described in Attachment A Snapchat Account **falyc0, phone number (206)434-0585, reported date of birth July 26, 2007, email address feylacow@outlook.com, IP Address 107.116.255.98** is within the possession, custody, or control of Snapchat, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Snapchat, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snapchat is required to disclose the following information to the government for the user listed in Attachment A for the dates of June 1, 2023, to the date of June 6, 2024[5]:

a. Subscriber basic contact information including subscriber, name, birth date, email address(es), physical address (city, state, zip, country), all telephone numbers, screen name and any associated website;

b. Basic subscriber information (BSI) including Subscriber Identification Number, Date and Time stamp of account creation date displayed in GMT, IP address at account sign-up, Logs in GMT showing source and destination IP addresses and ports; most recent Logins in GMT, registered mobile number(s), verification on whether publicly viewable, and all advertising identification number(s), as well as all devices used to access the account, including IMEI numbers, ICCID numbers, and all descriptions of make and model, and push-tokens;

c. Customer service records: All subscriber contacts with customer support including notifications or complaints of the account being hacked or stolen, or

[5] The date range commences from the date MV2 reported having communicated with "Josh" since the summer of 2023.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

any other issue with the use of or access to the Snapchat account that were created, uploaded, adjusted, accessed, used, modified, or deleted;

d. Subscriber financial account information and account status history;

e. Images: All photos, videos, and other depictions associated with the account, in any format or media. Law enforcement will search these files and only seize child pornography defined in in 18 U.S.C. § 2256, or files depicting self-mutilation or self-harm or torture, in addition to all depictions which demonstrate dominion and control over the account;

f. Postings, communications, biographical information, or other information identifying the suspect account user and/or any other persons transmitting depictions of minors engaged in sexually explicit conduct or evidencing the transmissions thereof;

g. Usage information detailing how the suspect account interacted with Snapchat including filters used to apply to Snaps, which Stories the suspect account watched on Discover, whether the suspect account used Spectacles, or which search queries the suspect account user submit;

h. Usage information detailing how the suspect account communicated with other Snapchatters, such as their names, the time and date of your communications, the number of messages exchanged with other users, which other users exchanged messages with the suspect account, and the suspect account's interactions with messages (such as when the suspect account opened a message or captured a screenshot);

i. Content information including information about the content created or provided by the suspect account, such as if the recipient has viewed the content and the metadata that is provided with the content;

j. Device information documenting the devices used by the suspect account to include information about the suspect account's hardware and software (to include hardware model, operating system version, device memory, advertising identifiers, unique application identifiers, apps installed, unique device identifiers, browser type, language, battery level, and time zone);

k. Device information documenting device sensors, such as accelerometers, gyroscopes, compasses, microphones, and whether the suspect account has headphones connected;

l. Device information documenting the wireless and mobile network connections, to include mobile phone number, service provider, IP address, and signal strength;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

m. Device information to include device Phonebook data collected, and any unique identifiers for devices used to access the account;

n. Device information to include Camera and Photos collected from the suspect account's device's camera and photos;

o. Location information about the suspect account's precise location using methods that include GPS, wireless networks, cell towers, Wi-Fi access points, and other sensors, such as gyroscopes, accelerometers, and compasses;

p. Information collected by cookies and other technologies to include information when the suspect account interacted with services Snapchat offers through one of its partners, such as advertising and commerce features;

q. Log information such as:

i. details about how the suspect account used Snapchat services;

ii. device information, such as the suspect account's web browser type and language;

iii. access times;

iv. pages viewed;

v. IP address;

vi. identifiers associated with cookies or other technologies that may uniquely identify the suspect account's device or browser; and

vii. pages the suspect account visited before or after navigating to Snapchat's website.

r. Information collected from Third Parties about the suspect account from other users, Snapchat affiliates, and third parties to include if the suspect account linked it's Snapchat account to another service (like Bitmoji or a third-party app) or if another user uploads their contact list, Snapchat may combine information from that user's contact list with other information Snapchat have collected about the suspect account.

Snapchat is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18 United States Code Section 2423(b) Travel with Intent to Engage in a Sexual Act with a Minor, Attempted Enticement of a Minor in violation of Title 18, United States Code, Section 2422(b), and violations of Title 18 United States Code Sections 2251(a)(4)(B), (b)(2), Possession of Child Pornography involving **falyc0, phone number (206)434-0585, reported date of birth July 26, 2007, email address feylacow@outlook.com, IP Address 107.116.255.98** in addition to unidentified suspects since the creation of the account, including, for each user ID identified on Attachment A, information pertaining to the following matters:

a. Evidence identifying the person(s) exercising dominion and control over the suspect account;

b. Financial account information and account status history;

c. Evidence indicating the targeting, communication, and solicitation of children to produce sexually explicit material, commit self-harm, or the exploitation and distribution of suicide videos at the direction of others;

d. All photos, videos, and other depictions associated with the account that depict child pornography defined in in 18 U.S.C. § 2256;

e. Images associated with the account belonging to the Snapchat suspect account user;

f. Postings, communications, biographical information, or other information identifying the suspect account user and/or any other persons transmitting depictions of minors engaged in sexually explicit conduct or evidencing the transmissions thereof;

g. Usage information evidence and communications from snapchat user **falyc0, phone number (206)434-0585, reported date of birth July 26, 2007, email address feylacow@outlook.com, IP Address 107.116.255.98** and others to include

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

communications to target minors for sexual and physical extortion or exploitation (including when the suspect account opened a message or captured a screenshot);

h. Evidence of payment for receipt of child sexual abuse material or material depicting self-harming or the harm of others;

i. Evidence indicating how and when the Snapchat account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Snapchat account owner;

j. Information about the content created or provided by the suspect account, when the content was viewed and the metadata that is provided with the content;

k. Data related to linked services;

l. User attribution evidence identifying the account user's devices, software, sensors, operating version, advertising identifiers, installed applications, unique identifiers, browser data, time zone, wireless and mobile network connections to include numbers, providers, IP addresses, and data related thereto;

m. Evidence of the Snapchat account user's state of mind as it relates to the crimes under investigation;

n. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s), and to establish dominion and control over the account during this time period.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970